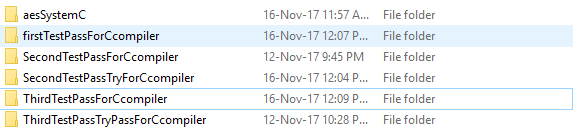
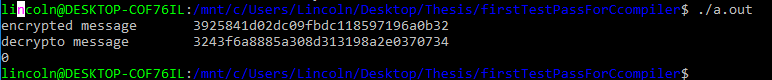
Στο φάκελος Thesis θα βρείτε κάποιες υλοποιήσεις του αλγορίθμου AES.

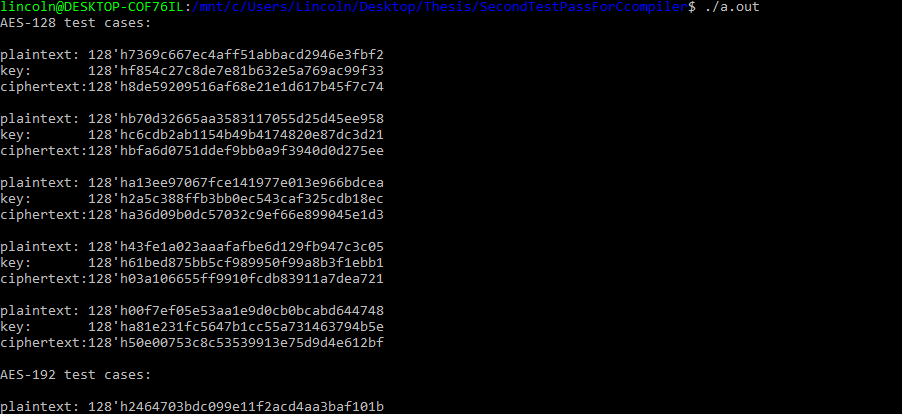
Το πρώτο είναι σε systemC , και τα άλλα είναι σε γλώσσα C.

Έτρεξα όλα αυτά που είναι σε γλώσσα C με την χρήση compiler μέσω command line gcc και μου βγάλανε όλα ένα output.

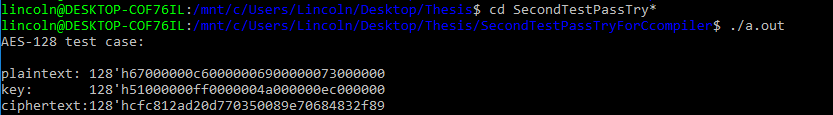
Για το 1ο:



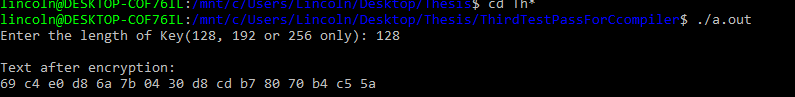
Για το 2ο:



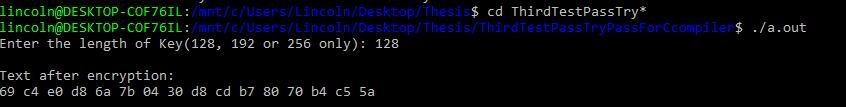
Για το 3ο:



Για το 4ο:

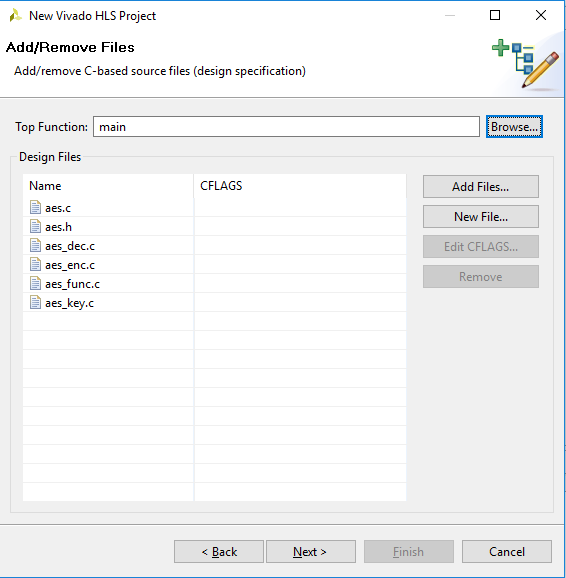


Για το 5ο:



Για το 1ο

Τοποθετώ τα αρχεία στο Vivado HLS



Πατάω synthesis και λαμβάνω ως αποτελέσματα:

WARNING: [HLS 200-40] Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:135:7: error: use of undeclared identifier 'word'

word[i][j] = key[i + j \* 4];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:144:23: error: use of undeclared identifier 'word'

temp[0] = SubByte (word[1][j - 1]) ^ Rcon0[(j / nk) - 1];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:145:23: error: use of undeclared identifier 'word'

temp[1] = SubByte (word[2][j - 1]);

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:146:23: error: use of undeclared identifier 'word'

temp[2] = SubByte (word[3][j - 1]);

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:147:23: error: use of undeclared identifier 'word'

temp[3] = SubByte (word[0][j - 1]);

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:151:14: error: use of undeclared identifier 'word'

temp[0] = word[0][j - 1];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:152:14: error: use of undeclared identifier 'word'

temp[1] = word[1][j - 1];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:153:14: error: use of undeclared identifier 'word'

temp[2] = word[2][j - 1];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:154:14: error: use of undeclared identifier 'word'

temp[3] = word[3][j - 1];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:160:2: error: use of undeclared identifier 'word'

word[i][j] = word[i][j - nk] ^ temp[i];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:160:15: error: use of undeclared identifier 'word'

word[i][j] = word[i][j - nk] ^ temp[i];

^

11 errors generated.

ERROR: [HLS 200-70] Compilation errors found:

Pragma processor failed: Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:135:7: error: use of undeclared identifier 'word'

word[i][j] = key[i + j \* 4];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:144:23: error: use of undeclared identifier 'word'

temp[0] = SubByte (word[1][j - 1]) ^ Rcon0[(j / nk) - 1];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:145:23: error: use of undeclared identifier 'word'

temp[1] = SubByte (word[2][j - 1]);

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:146:23: error: use of undeclared identifier 'word'

temp[2] = SubByte (word[3][j - 1]);

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:147:23: error: use of undeclared identifier 'word'

temp[3] = SubByte (word[0][j - 1]);

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:151:14: error: use of undeclared identifier 'word'

temp[0] = word[0][j - 1];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:152:14: error: use of undeclared identifier 'word'

temp[1] = word[1][j - 1];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:153:14: error: use of undeclared identifier 'word'

temp[2] = word[2][j - 1];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:154:14: error: use of undeclared identifier 'word'

temp[3] = word[3][j - 1];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:160:2: error: use of undeclared identifier 'word'

word[i][j] = word[i][j - nk] ^ temp[i];

^

Desktop/Thesis/firstTestPassForCcompiler/aes\_key.c:160:15: error: use of undeclared identifier 'word'

word[i][j] = word[i][j - nk] ^ temp[i];

^

11 errors generated.

Failed checking during preprocessing.

while executing

"source C:/Users/Lincoln/fIRST/solution1/csynth.tcl"

invoked from within

"hls::main C:/Users/Lincoln/fIRST/solution1/csynth.tcl"

("uplevel" body line 1)

invoked from within

"uplevel 1 hls::main {\*}$args"

(procedure "hls\_proc" line 5)

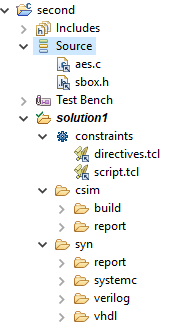
invoked from within

"hls\_proc $argv"

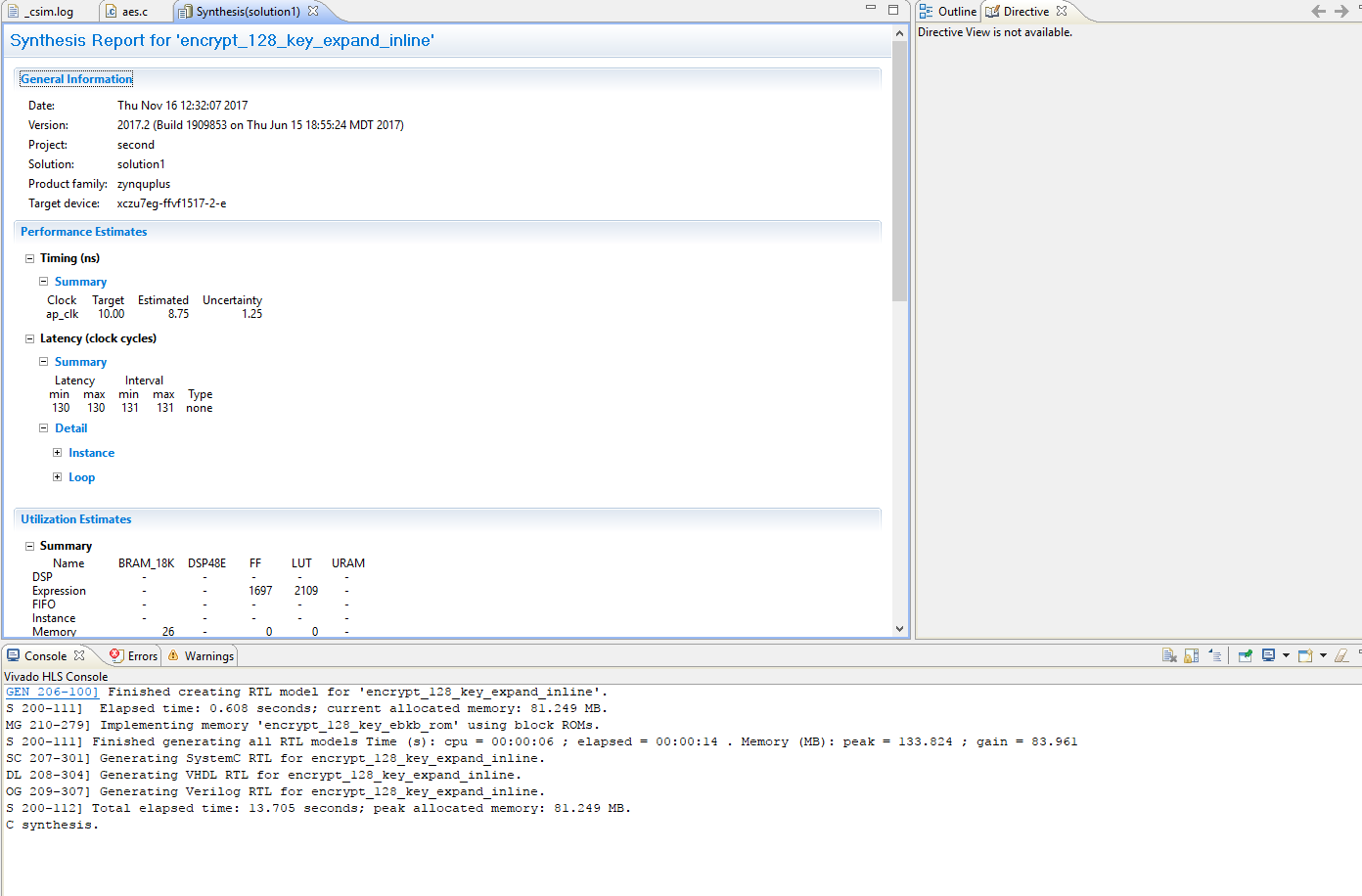
Finished C synthesis.

Βάζω το 2ο test:

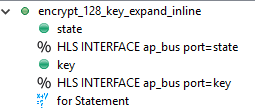
Έχω αυτά τα αρχεία:



Κάνω synthesis και μου βγάζει :



Οι αλλαγές που έκανα είναι ότι έβαλα το key και το state interface με ap\_bus

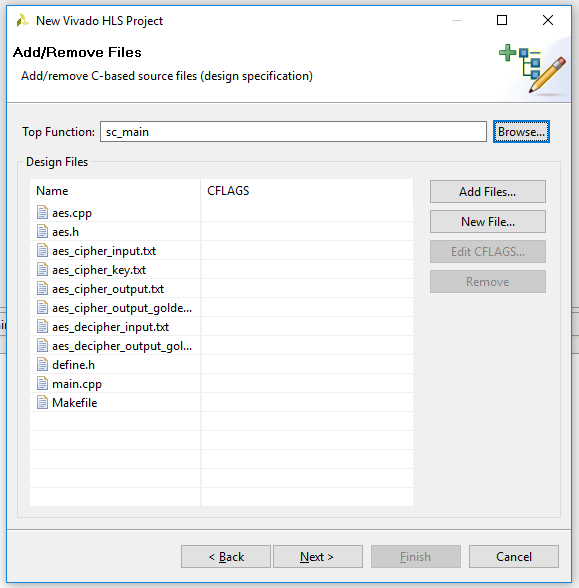


3ο  test:

Δεν ξέρω ποια αρχεία να βάλω για να τα κάνω synthesis

SystemC αρχείο:

Βάζω αυτά τα αρχεία:



Και μου βγάζει στην σύνθεση αυτά:

WARNING: [HLS 200-40] In file included from C:/Users/Lincoln/Csysteacffac/solution1/.autopilot/db/main.pragma.1.cpp:1:

In file included from Desktop/Thesis/aesSystemC/aes\_combined/main.cpp:1:

Desktop/Thesis/aesSystemC/aes\_combined/main.cpp:26:3: error: use of undeclared identifier 'sc\_clock'

sc\_clock clk("clk", 25, SC\_NS, 0.5, 12.5, SC\_NS, true);

^

Desktop/Thesis/aesSystemC/aes\_combined/main.cpp:42:14: error: use of undeclared identifier 'clk'

u\_AES.clk( clk );

^

Desktop/Thesis/aesSystemC/aes\_combined/main.cpp:54:13: error: use of undeclared identifier 'clk'

test.clk( clk );

^

Desktop/Thesis/aesSystemC/aes\_combined/main.cpp:88:16: error: use of undeclared identifier 'SC\_NS'

sc\_start( 25, SC\_NS );

^

Desktop/Thesis/aesSystemC/aes\_combined/main.cpp:93:17: error: use of undeclared identifier 'SC\_NS'

sc\_start( 25, SC\_NS );

^

Desktop/Thesis/aesSystemC/aes\_combined/main.cpp:97:18: error: use of undeclared identifier 'SC\_NS'

sc\_start(1000, SC\_NS);

^

Desktop/Thesis/aesSystemC/aes\_combined/main.cpp:98:3: error: use of undeclared identifier 'sc\_start'

sc\_start();

^

7 errors generated.

Compilation of the preprocessed source 'main.g' failed

while executing

"source C:/Users/Lincoln/Csysteacffac/solution1/csynth.tcl"

invoked from within

"hls::main C:/Users/Lincoln/Csysteacffac/solution1/csynth.tcl"

("uplevel" body line 1)

invoked from within

"uplevel 1 hls::main {\*}$args"

(procedure "hls\_proc" line 5)

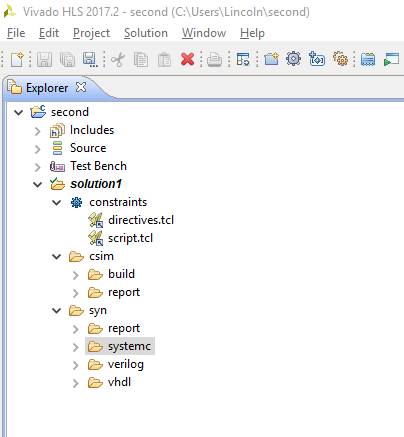
invoked from within

"hls\_proc $argv"

Finished C synthesis.

Μάλλον επειδή δεν κάνει σειριακά compile και όχι όλα μαζί.

Στο 2ο παράδειγμα από τι βλέπετε:



Έβγαλε και ένα αρχείο από την synthesis σε γλώσσα systemC.

Μήπως το πρόγραμμα κάνει σύνθεση μόνο από C/C++ σε γλώσσα VHDL, Verilog, SystemC ;